

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH (1)
BLACLOUD21@AOL.COM, (2)
THESNEEK14@AOL.COM, and (3)
HIDENSNEEK14@AIM.COM THAT IS
STORED AT PREMISES CONTROLLED BY
APPLE, INC.

16-780 M

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, CHANCE J. ADAM, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the above-captioned Apple IDs that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) for approximately nine and a half years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for racketeering and other crimes associated with organized crime, and, in particular, the five organized crime families collectively known as “La Cosa Nostra.” These investigations are conducted both overtly and covertly. I have participated in investigations involving search warrants and arrest

warrants, and well as confidential informants and cooperating witnesses. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. I have participated in investigations involving search warrants and arrest warrants, including tracking warrants and phone location information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. The FBI, the New York City Police Department (“NYPD”), together with the United States Attorney’s Office for the Eastern District of New York, are conducting an investigation into the circumstances surrounding the June 30, 2016 murder of Louis Barbatì for possible violations of Title 18, United States Code, Section 1951 (attempted Hobbs Act Robbery, Hobbs Act Robbery conspiracy, and committing or threatening physical violence in connection with such a violation), Title 18, United States Code, Section 924(j) (firearm-related murder), Title 18, United States Code, Section 1958 (murder for hire), and Title 18, United States Code, Section 1959 (murder in-aid-of racketeering), among other possible violations of law. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence and/or instrumentalities of violations of these offenses, as described in Attachment B.

PROBABLE CAUSE

I. Background of La Cosa Nostra

5. La Cosa Nostra operates through organized crime families. Five of these crime families – the Bonanno, Colombo, Gambino, Genovese and Lucchese crime families – are headquartered in New York City, and supervise criminal activity in New York, in other areas of the United States and, in some instances, in other countries. The principal purpose of La Cosa Nostra is to generate money for its members and associates. This purpose is implemented by members and associates of La Cosa Nostra through various criminal activities, including robbery, extortion, illegal gambling and loansharking. La Cosa Nostra members and associates also further the enterprise's criminal activities by threatening economic injury and using and threatening to use physical violence, including murder.

6. Although the primary purpose of La Cosa Nostra is to generate money for its members and associates, the members and associates at times use the resources of the family to settle personal grievances and vendettas, sometimes with the approval of higher-ranking members of the family. For those purposes, members and associates of the enterprise are asked and expected to carry out, among other crimes, acts of violence, including murder, extortion, robbery and assault.

II. 2010 La Cosa Nostra Dispute Involving L&B Spumoni Gardens

7. L&B Spumoni Gardens ("L&B") has, historically, been the subject of a dispute involving La Cosa Nostra. A cooperating witness ("CW") has advised about a 2010 dispute

involving L&B and individuals associated with Colombo and Bonanno crime families.¹

According to the CW, in 2010, Colombo family associate Francis Guerra's wife's parents were part owners of L&B, an Italian restaurant in Brooklyn, New York. The children of Eugene Lombardo, a Bonanno family associate, worked at L&B. Subsequently, Lombardo opened a pizzeria on Staten Island called "The Square," and Guerra came to believe that Lombardo had stolen a sauce recipe from L&B.

8. In the summer of 2010, Guerra, the CW, who, at the time, was an inducted member of the Colombo family, and a Colombo family associate Frank "Frankie Notch" Iannaci went to The Square and bought a pizza. When they saw Lombardo in front of the pizzeria, Iannaci assaulted him and Guerra yelled, "How could you disrespect my family?"

¹ In the 1980s, the CW was an associate of the Gambino crime family. Beginning in or before 1992, he became an associate of the Colombo crime family. He was inducted into the Colombo crime family in 2009 and subsequently became an acting captain in that crime family. In 2011, he pled guilty in the Eastern District of New York, pursuant to a cooperation agreement, to racketeering conspiracy, including as racketeering acts murder, extortion and loansharking. The CW subsequently testified at trial against a Colombo family associate, and, after the government filed a motion pursuant to U.S.S.G. § 5K1.1, he was sentenced to a total term of imprisonment of approximately 34 months. In addition, the CW's criminal history includes, prior to his 2011 conviction, convictions in the 1980s for firearms possession and assault, and a conviction in 2000 for using a communications facility to commit a narcotics felony. The 2000 conviction resulted in a 96-month term of imprisonment imposed in the Southern District of New York. The CW has also admitted to participating in insurance fraud, robberies, accessory-after-the-fact to murder, assault, murder conspiracy, witness tampering, tax evasion, and carrying a firearm in connection with a crime of violence. The CW's information has been extensively corroborated by other cooperating witness, surveillances, crime-scene evidence, documentary evidence and recorded conversations, among other sources of evidence.

9. Bonanno crime family member Anthony Calabrese then looked for the CW. The CW and Calabrese met at St. Joseph's high school on Hylan Boulevard in Staten Island. The CW told Calabrese that Lombardo would have to make him and Guerra partners in The Square or close the place down.

10. Benjamin Castellazzo, who at the time of the dispute was the underboss of the Colombo crime family, learned about the assault of Lombardo from Ralph DiMatteo, a partner in The Square who was "on record" with Castellazzo. Castellazzo met with the CW, and approved Guerra's and the CW's efforts to obtain a portion of the proceeds of The Square, provided that they give a portion of any proceeds to Castellazzo. A week later, the CW met with Calabrese and others. They agreed that Lombardo would provide \$3,000 to \$4,000 as a one-time payment. A few days later, the CW collected the money from Calabrese. The CW and Guerra split the money and gave \$500 to Castellazzo, whom they had kept apprised of the situation, because of DiMatteo's involvement in The Square.

11. Louis Barbati, whose grandfather began the business, was a co-owner of L&B at the time of this dispute and remained a co-owner until he was killed on June 30, 2016.

III. The Murder of Louis Barbati

12. On June 30, 2016, at approximately 7:02 p.m., Louis Barbati, was shot several times and killed as he walked from his car to his house, located at 7601 12th Avenue, in the Dyker Heights section of Brooklyn, New York. Mr. Barbati had left L&B earlier that evening at approximately 6:30 p.m. Mr. Barbati was carrying more than \$10,000 in cash at the time he was killed, which represented proceeds from L&B.

13. Based on their review of video surveillance footage collected from the vicinity of the murder, before and around the time the murder was committed, law enforcement officers

have identified an individual wearing shorts, a dark hooded sweatshirt and sunglasses as the primary suspect in the murder of Mr. Barbati. The review of surveillance footage revealed that the same individual was observed, at times seated inside a white, late-model Acura with New York plates that was parked in front of a fire hydrant across the street from Mr. Barbati's home, beginning at approximately 5:30 p.m. The review of surveillance footage also revealed images of the man walking up and down the block before the murder and indicated that the man repeatedly used a cellular telephone as he waited.

14. A civilian witness from the neighborhood observed the man in the hooded sweatshirt and shorts leaving the vicinity of the murder in a white, late-model Acura. The review of the surveillance footage revealed, similarly, that after the murder, the same man entered the driver's side door of the Acura, and drove away at approximately 7:02 p.m.

15. Approximately four seconds after the Acura pulled away, Mr. Barbati's wife can be observed leaving the back door of their home and approaching the vicinity of his body.

16. Law enforcement officers recovered three cigarette butts from the vicinity of where the white Acura was observed parked at the fire hydrant. Male DNA suitable for DNA comparison was recovered from each of the three cigarette butts.

17. Subsequent to the murder, the NYPD distributed portions of the surveillance video referenced above to the public. Multiple individuals have anonymously contacted the NYPD in response and identified the man depicted in the surveillance video as Andres Fernandez, also known as "Andy Fernandez."

18. Law enforcement officers have also reviewed records from the New York State Department of Motor Vehicles, which indicate that a white 2014 Acura TL with New York

license plate number GME8687 is registered to Andres Fernandez with a date of birth of August 19, 1975.

19. I have reviewed a copy of an arrest photograph associated with Andres Fernandez with date of birth August 19, 1975, and I have compared it to still images from the surveillance video referenced above. The individual depicted in the surveillance video described above appears, in fact, to be Andres Fernandez.

20. On August 14, 2015, the NYPD arrested Andres Fernandez pursuant to an outstanding warrant for an assault. According to law enforcement reports created in connection with that arrest, Andres Fernandez's cellular telephone number at the time of his arrest was (917) 952-1578 (the "Fernandez Cell Phone").

21. Based on telephone records I have reviewed that were provided by Verizon pursuant to a grand jury subpoena, I know that on June 30, 2016, the Fernandez Cell Phone was serviced by Verizon and was subscribed in the name of Andres Fernandez. According to those records and a Verizon representative, the Fernandez Cell Phone was assigned to an Apple iPhone 6 with MEID a0000053dd98f6.²

22. Location information obtained from Verizon Wireless pursuant to a court-authorized search warrant for the Fernandez Cell Phone revealed that the Fernandez Cell Phone used cell towers that provided cellular service to 7601 12th Avenue, the location of the murder, in the time leading up to Mr. Barbati's murder. In addition, according to these records, prior to the murder, at the time the Fernandez Cell Phone was connected to those cell towers, it was

² According to a Verizon representative, the company's records sometimes describe a device's MEID as an electronic serial number ("ESN"), an older form of mobile device identification that existed prior to the MEID system.

connected to an Internet Protocol (“IP”) address owned by Apple Inc., indicating that the user of the Fernandez Cell Phone may have been using Apple Inc. products or services to communicate with others.

23. Records obtained from Apple Inc. pursuant to an order under 18 U.S.C. § 2703(d) issued by the Honorable Roanne L. Mann, United States Magistrate Judge, Eastern District of New York, revealed that the Fernandez Cell Phone initiated calls using Apple’s FaceTime service in the days before and after the murder. The records also revealed that (1) Apple ID “blaccloud21@aol.com” is registered to “Andres Fernandez” with an address of “3020 avey [sic], Brooklyn, New York;” (2) Apple ID “thesneek14@aol.com” is registered to “Andy Fernandez” with an address of “3020 ave y, Brooklyn, New York;” and (3) Apple ID “hidensneek14@aim.com” is registered to “Andres Fernandez” with an address of “3020 ave Y apt 8J, Brooklyn, New York.”

24. Andres Fernandez’s New York State driver’s license lists an address of 3020 Avenue Y, Apt. 7E, Brooklyn, New York 11235. An application for a rollover IRA account for Andres Fernandez lists an address of 3020 Avenue Y, Apt. 8J, Brooklyn, New York 11235.

25. On July 19, 2016, pursuant to Title 18, United States Code, Section 2703(d), Apple Inc. was requested to preserve all stored communications, records, and other evidence in its possession regarding accounts associated with the Apple IDs blaccloud21@aol.com, thesneek14@aol.com, and hidensneek14@aim.com.

INFORMATION REGARDING APPLE ID AND iCloud³

26. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

27. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

³ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS Security,” available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be

purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

28. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

29. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as AOL, AIM, Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

30. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the IP address used to register and access the account, and other log files that reflect usage of the account.

31. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

32. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

33. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

34. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, probably will be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

35. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

36. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

37. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

39. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information probably will constitute evidence of the crimes under investigation, including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

40. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant.

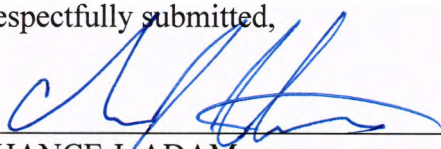
42. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

44. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



CHANCE J. ADAM
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 23, 2016



HON. RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple IDs (1) blacloud21@aol.com, (2) thesneek14@aol.com, and (3) hidensneek14@aim.com (each, an “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Section 1951, Title 18, United States Code, Section 924(j), Title 18, United States Code, Section 1958, and Title 18, United States Code, Section 1959 involving Andres Fernandez since June 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The murder of Louis Barbati;
- b. Preparatory steps taken in furtherance of the scheme resulting in Louis Barbati's murder;
- c. Associations with La Cosa Nostra or other organized crime organizations;
- d. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- e. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- f. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- g. Evidence indicating the subscriber's state of mind as it relates to the murder of Louis Barbati; and

h. Evidence, including communications, that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature